Congressional Research Service
Informing the legislative debate since 1914

Cyberwarfare and Cyberterrorism: In Brief

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

John W. Rollins
Specialist in Terrorism and National Security

March 27, 2015

Congressional Research Service
7-5700
www.crs.gov
R43955

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Recent incidents have highlighted the lack of consensus internationally on what defines a cyberattack, an act of war in cyberspace, or cyberterrorism. Cyberwar is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies. Within each of these categories, different motivations as well as overlapping intent and methods of various actors can complicate response options.

Criminals, terrorists, and spies rely heavily on cyber-based technologies to support organizational objectives. Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain. Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives. Cyberactivists are individuals who perform cyberattacks for pleasure, philosophical, political, or other nonmonetary reasons.

There are no clear criteria yet for determining whether a cyberattack is criminal, an act of hactivism, terrorism, or a nation-state's use of force equivalent to an armed attack. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace.

The current domestic legal framework surrounding cyberwarfare and cyberterrorism is equally complicated. Authorizations for military activity in cyberspace contain broad and undefined terms. There is no legal definition for cyberterrorism. The USA PATRIOT Act's definition of terrorism and references to the Computer Fraud and Abuse Act appear to be the only applicable working construct. Lingering ambiguities in cyberattack categorization and response policy have caused some to question whether the United States has an effective deterrent strategy in place with respect to malicious activity in cyberspace.

Contents

Contacts

Introduction

"Cyberattack" is a relatively recent term that can refer to a range of activities conducted through the use of information and communications technology (ICT). The use of distributed denial of service (DDoS) attacks has become a widespread method of achieving political ends through the disruption of online services. In these types of attacks, a server is overwhelmed with Internet traffic so access to a particular website is degraded or denied. The advent of the Stuxnet worm, which some consider the first cyberweapon, showed that cyberattacks may have a more destructive and lasting effect. Appearing to target Iran, Stuxnet malware attacked the computerized industrial control systems on which nuclear centrifuges operate, causing them to self-destruct.

Recent international events have raised questions on when a cyberattack could be considered an act of war, and what sorts of response options are available to victim nations. Although there is no clear doctrinal definition of "cyberwarfare," it is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies.

The cyberattacks on Sony Entertainment illustrate the difficulties in categorizing attacks and formulating a response policy. On November 24, 2014, Sony experienced a cyberattack that disabled its information technology systems, destroyed data and workstations, and released internal emails and other materials. Warnings surfaced that threatened "9/11-style" terrorist attacks on theaters scheduled to show the film *The Interview*, causing some theaters to cancel screenings and for Sony to cancel its widespread release, although U.S. officials claimed to have "no specific, credible intelligence of such a plot." The Federal Bureau of Investigation (FBI) and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government; North Korea denied involvement in the attack, but praised a hacktivist group, called the "Guardians of Peace," for having done a "righteous deed." During a December 19, 2014, press conference, President Obama pledged to "respond proportionally" to North Korea's alleged cyber assault, "in a place, time and manner of our choosing." President Obama referred to the incident as an act of "cyber-vandalism," while others decried it as an act of cyberwar.

This incident illustrates challenges in cyberattack categorization, particularly with respect to the actors involved and their motivations as well as issues of sovereignty regarding where the actors were physically located. With the globalized nature of the Internet, perpetrators can launch cyberattacks from anywhere in the world and route the attacks through servers of third-party countries. Was the cyberattack on Sony, a private corporation with headquarters in Japan, an attack on the United States? Further, could it be considered an act of terrorism, a use of force, or cybercrime? In categorizing the attacks on Sony as an act of "cyber vandalism," which typically includes defacing websites and is usually the realm of politically motivated actors known as "hacktivists," President Obama raised questions of what type of response could be considered "proportional," and against whom. Another potential policy question could be the circumstances under which the United States would commit troops to respond to a cyberattack. Related to this is the question of whether the U.S. has an effective deterrence strategy in place. According to DNI

Clapper, "If they get global recognition at a low cost and no consequence, they will do it again and keep doing it again until we push back."[1]

The Cyberwarfare Ecosystem: A Variety of Threat Actors

Criminals, terrorists, and spies rely heavily on cyber-based technologies to support organizational objectives. Commonly recognized cyber-aggressors and representative examples of the harm they can inflict include the following:

Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, and a means of communication, and for disruptive purposes.[2] While no unclassified reports have been published regarding a cyberattack on a critical component of U.S. infrastructure, the vulnerability of critical life-sustaining control systems being accessed and destroyed via the Internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed.[3] Cyberterrorists may be seeking a destructive capability to exploit these vulnerabilities in critical infrastructure.

Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. Targets include government networks, cleared defense contractors, and private companies. For example, a 2011 FBI report noted, "a company was the victim of an intrusion and had lost 10 years' worth of research and development data—valued at $1 billion—virtually overnight."[4] Likewise, in 2008 the Department of Defense's (DOD) classified computer network system was unlawfully accessed and "the computer code, placed there by a foreign intelligence agency, uploaded itself undetected onto both classified and unclassified systems from which data could be transferred to servers under foreign control."[5]

Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain. Examples include an organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a

[1] See http://www.bloomberg.com/politics/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.

[2] For additional information, see CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

[3] See "Challenges Remain in DHS' Efforts to Security Control Systems," Department of Homeland Security, Office of Inspector General, August 2009. For a discussion of how computer code may have caused the halting of operations at an Iranian nuclear facility see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[4] Executive Assistant Director Shawn Henry, *Responding to the Cyber Threat*, Federal Bureau of Investigation, Baltimore, MD, 2011.

[5] Department of Defense Deputy Secretary of Defense William J. Lynn III, "Defending a New Domain," Foreign Affairs, October 2010.

financial account. One estimate has placed the annual cost of cybercrime to individuals in 24 countries at $388 billion.[6] However, given the complex and sometimes ambiguous nature of the costs associated with cybercrime, and the reluctance in many cases of victims to admit to being attacked, there does not appear to be any publicly available, comprehensive, reliable assessment of the overall costs of cyberattacks.

Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives.[7] These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyberattack and are often blamed by the host country when accusations are levied by the nation that has been attacked. Often, when a foreign government is provided evidence that a cyberattack is emanating from its country, the nation that has been attacked is informed that the perpetrators acted of their own volition and not at the behest of the government. In August 2012 a series of cyberattacks were directed against Saudi Aramco, the world's largest oil and gas producer. The attacks compromised 30,000 computers and the code was apparently designed to disrupt or halt oil production. Some security officials have suggested that Iran may have supported this attack. However, numerous groups, some with links to nations with objectives counter to Saudi Arabia, have claimed credit for this incident.

Cyberactivists are individuals who perform cyberattacks for pleasure, philosophical, political, or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist" such as a member of the cyber-group Anonymous who undertakes an attack for political reasons. The activities of these groups can range from nuisance-related denial of service attacks and website defacement to disrupting government and private corporation business processes.

The threats posed by these cyber-aggressors and the types of attacks they can pursue are not mutually exclusive. For example, a hacker targeting the intellectual property of a corporation may be categorized as both a cyberthief and a cyberspy. A cyberterrorist and cyberwarrior may be employing different technological capabilities in support of a nation's security and political objectives. Some reports indicate that cybercrime has now surpassed the illegal drug trade as a source of funding for terrorist groups, although there is some confusion as to whether a particular action should be categorized as cybercrime.[8] Ascertaining information about an aggressor and its capabilities and intentions is difficult.[9] The threats posed by these aggressors coupled with the United States' proclivity to be an early adopter of emerging technologies,[10] which are often

[6] For discussions of federal law and issues relating to cybercrime, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, and CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[7] For additional information, see CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary.

[8] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar,* RAND. For more information on cybercrime definitions, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

[9] The concept of attribution in the cyber world entails an attempt to identify with some degree of specificity and confidence the geographic location, identity, capabilities, and intention of the cyber-aggressor. Mobile technologies and sophisticated data routing processes and techniques often make attribution difficult for U.S. intelligence and law enforcement communities.

[10] Emerging cyber-based technologies that may be vulnerable to the actions of a cyber-aggressor include items that are in use but not yet widely adopted or are currently being developed. For additional information on how the convergence (continued...)

interdependent and contain vulnerabilities, makes for a complex environment when considering operational responses, policies, and legislation designed to safeguard the nation's strategic economic and security interests.

Cyberwarfare

There are no clear criteria yet for determining whether a cyberattack is criminal, an act of hactivism, terrorism, or a nation-state's use of force equivalent to an armed attack. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace. In September 2012, the State Department took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the U.N. Charter and customary international law. According to State's then-legal advisor, Harold Koh, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[11] Examples offered in Koh's remarks included triggering a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control. By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyberwar fits easily within existing international legal frameworks. If an actor employs a cyberweapon to produce kinetic effects that might warrant fire power under other circumstances, then the use of that cyberweapon rises to the level of the use of force.

However, the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances. Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, "computer network activities that amount to an armed attack or imminent threat thereof" may trigger a nation's right to self-defense under Article 51 of the U.N. Charter. Koh cites in his remarks the 2011 *International Strategy for Cyberspace*,[12] which affirmed that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." The *International Strategy* goes on to say that the U.S. reserves the right to use all means necessary—diplomatic, informational, military, and economic—as appropriate and consistent with applicable law, and exhausting all options before military force whenever possible.

Rules of the Road and Norm-Building in Cyberspace

One of the defense objectives of the *International Strategy for Cyberspace* is to work internationally "to encourage responsible behavior and oppose those who would seek to disrupt

(...continued)

of inexpensive, highly sophisticated, and easily accessible technology is providing opportunities for cyber-aggressors to exploit vulnerabilities found in a technologically laden society see *Global Trends 2030: Alternative Worlds, National Intelligence Council*, Office of the Director of National Intelligence, December 10, 2012.

[11] Remarks of Harold Hongju Koh, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

[12] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

networks and systems, dissuading and deterring malicious actors, and reserving the right to defend national assets." A growing awareness of the threat environment in cyberspace has led to two major international processes geared toward developing international expert consensus among international cyber authorities.

A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia. The CCDCOE hosts workshops and courses on law and ethics in cyberspace, as well as cyber defense exercises. In 2009, the center convened an international group of independent experts to draft a manual on the law governing cyberwarfare. The *Tallinn Manual*, as it is known, was published in 2013.[13] It sets out 95 "black letter rules" governing cyber conflict addressing sovereignty, state responsibility, the law of armed conflict, humanitarian law, and the law of neutrality. The *Tallinn Manual* is an academic text: although it offers reasonable justifications for the application of international law, it is non-binding and the authors stress that they do not speak for NATO or the CCDCOE.

In the provisions of Article 5 of the North Atlantic Treaty, an attack on one member is considered an attack on all, affording military assistance in accordance with Article 51 of the United Nations Charter. However, NATO does not presently define cyberattacks as clear military action. The *Tallinn Manual* equates a use of force to those cyber operations whose "effects ... were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack." Article 4 of the North Atlantic Treaty applies the principles of collective consultation to any member state whose security and territorial integrity has been threatened; however it is unclear how this would apply to the various categories of cyberattacks, some of which may not have kinetic equivalents. If an attack is deemed to be orchestrated by a handful of cyber criminals, whether politically or financially motivated, then it may fall upon the attacked state to determine the appropriate response within its jurisdiction. However the transnational nature of most criminal organizations in cyberspace can complicate decisions of jurisdiction.

Law of Armed Conflict

Reprisals for armed attacks are permitted in international law when a belligerent violates international law during peacetime, or the law of armed conflict during wartime. However, the term "armed attack" has no legal definition and is still open to interpretation with respect to cyberattacks. The so-called "Law of War," also known as the law of armed conflict, embodied in the Geneva and Hague Conventions and the U.N. Charter may in some circumstances apply to cyberattacks, but without attempts by nation states to apply it, or specific agreement on its applicability, its relevance remains unclear. It is also complicated by difficulties in attribution, the potential use of remote computers, and possible harm to third parties from cyber counterattacks, which may be difficult to contain. In addition, questions of territorial boundaries and what constitutes an armed attack in cyberspace remain. The law's application would appear clearest in situations where a cyberattack causes physical damage, such as disruption of an electric grid. As mentioned above, the *Tallinn Manual* addresses many of these questions.[14] In the absence of a

[13] Tallinn Manual on the International Law Applicable to Cyber Warfare, available at https://ccdcoe.org/tallinn-manual.html.

[14] For a detailed discussion, see Hathaway et al., "The Law of Cyber-Attack." See also CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary; James A. Lewis, *Conflict and Negotiation in Cyberspace* (Center for Strategic and International Studies, February 2013), https://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf; Mary Ellen O'Connell and Louise Arimatsu, *Cyber Security and International Law* (London, UK: Chatham House, May 29, 2012), http://www.tsa.gov/sites/default/files/assets/pdf/ (continued...)

legal definition for what constitutes an "armed attack" in cyberspace, Professor Michael Schmitt has proposed criteria for analysis under international law:[15]

Severity: Perhaps the most significant factor in the analysis, consequences involving physical harm to individuals or property will alone amount to a use of force while those generating only minor inconvenience or irritation will not. The more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force.

Immediacy: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.

Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force.

Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one state cross into another in violation of its sovereignty. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory.

Measurability: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. This is particularly challenging in a cyber event, where damage, economic or otherwise, is difficult to quantify. Economic coercion or hardship does not qualify under international law as an armed attack.

Presumptive legitimacy: In international law, acts which are not forbidden are permitted; absent an explicit prohibition, an act is presumptively legitimate. For instance, it is generally accepted that international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

Responsibility: The law of state responsibility governs when a state will be responsible for cyber operations. However that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability. Attributing the level of state involvement to a cyberattack can be particularly challenging.

(...continued)

Intermodal/pipeline_sec_incident_recvr_protocol_plan.pdf.

[15] This section has been adapted from M.N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revised", Vol. 56 *Villanova Law Review* 2011, at p. 576 *et seq*.; M. N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context" and K Ziolkowski, "Ius ad bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force" in the 2012 4th *International Conference on Cyber Conflict,* C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)

The basic principles encompassed in the Hague Conventions regarding the application of Armed Forces are those of military necessity, proportionality, humanity and chivalry. If a nation's military is conducting cyber operations according to these principles, it may be said to be engaging in cyberwar.

Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime[16] is the first international treaty to attempt to harmonize laws across countries as to what constitutes criminal activity in the cyber realm. This law enforcement treaty, also known as the Budapest Convention, requires signatories to adopt criminal laws against specified types of activities in cyberspace, to empower law enforcement agencies to investigate such activities, and to cooperate with other signatories. While widely cited as the most substantive international agreement relating to cybersecurity, some observers regard it as unsuccessful.[17] Critics warn that the Convention is short on the enforcement side, and lacks jurisdiction in countries where criminals operate freely. In addition to most members of the Council of Europe, the United States and three other nations have ratified the treaty.[18]

United Nations General Assembly Resolutions

A series of U.N. General Assembly resolutions relating to cybersecurity have been adopted over the past 15 years. One resolution called for the convening of and a report from an international group of government experts from 15 nations, including the United States. The stated purpose of this process was to build "cooperation for a peaceful, secure, resilient and open ICT environment" by agreeing upon "norms, rules and principles of responsible behaviour by States" and identifying confidence and capacity-building measures, including for the exchange of information. Unlike the work done at Tallinn under the auspices of NATO, this U.S.-led process included both China and Russia. The resulting 2010 report, sometimes referred to as the Group of Governmental Experts (GGE) Report, recommended a series of steps to "reduce the risk of misperception resulting from ICT[19] disruptions" but did not incorporate any binding agreements.[20] Nevertheless, some observers believe the report represents progress in overcoming differences between the United States and Russia about various aspects of cybersecurity.[21] In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society (WSIS) to discuss information society opportunities and challenges. This summit was

[16] See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[17] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" *Future Challenges Essay*, June 2, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf. He cites "vague definitions," reservations by signatories, and loopholes as reasons for its lack of success.

[18] Council of Europe, "Convention on Cybercrime, CETS No. 185," accessed February 18, 2013, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. See also Michael Vatis, "The Council of Europe Convention on Cybercrime," in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (Washington, DC: National Academies Press, 2010), pp. 207–223.

[19] The abbreviation ICT, which stands for information and communications technologies, is increasingly used instead of IT, (information technologies) because of the convergence of telecommunications and computer technology.

[20] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, July 30, 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

[21] Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review 100*, no. 4 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.

first convened in Geneva, in 2003, and then in Tunis, in 2005, and a10-year follow-on in Geneva in May 2013. Delegates from 175 countries took part in the first summit, where they adopted a Declaration of Principles—a road map for achieving an open information society. The Geneva summit left other, more controversial issues unresolved, including the question of Internet governance and funding. At both summits, proposals for the United States to relinquish control of the Internet Corporation for Assigned Names and Numbers (ICANN) were rejected.

An international treaty banning cyberwarfare and/or information weapons has been proposed in the United Nations by Russian and German delegations. Preferring a normative approach over an arms control styled regime, the United States may wish to reserve its right to develop technologies for countermeasures and reconnaissance against potential cyber foes, particularly those acting outside the boundaries of a state system.

International Telecommunications Regulations

The International Telecommunication Union (ITU) regulates international telecommunications through binding treaties and regulations and nonbinding standards. Regulations prohibit interference with other nations' communication services and permit control of non-state telecommunications for security purposes. The regulations do not, however, expressly forbid military cyberattacks. Also, ITU apparently has little enforcement authority.[22]

The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, during December 3-14, 2012, to review the International Telecommunications Regulations. In the run-up to the summit, many security observers expressed concern over the closed nature of the talks and feared a shift of Internet control away from private entities such as ICANN toward the United Nations and national governments. Although these concerns proved to be largely baseless, a controversial deep packet inspection proposal from the People's Republic of China was adopted at the summit.[23] Dissenting countries, including Germany, fear that this recommendation will result in accelerated Internet censorship in repressed nations.

Other International Law

Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cybersecurity; for example by prohibiting the disruption of air traffic control or other conduct that might jeopardize aviation safety.[24] Bilaterally, mutual legal assistance treaties between countries may be applicable for cybersecurity forensic investigations and prosecution.

The United States has signed at least 16 treaties and other agreements with 13 other countries and the European Union that include information security, classified military information, or defense-related information assurance and protection of computer networks. According to news reports,

[22] Hathaway et al.,"The Law of Cyber-Attack." See also Anthony Rutkowski, "Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850," Info 13, no. 1 (2011): 13–31, http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=13&issue=1&articleid=1893240&show=pdf&PHPSESSID=9r0c5maa4spkkd9li78ugbjee3.

[23] Deep packet inspection allows the content of a unit of data to be examined as it travels through an inspection point, a process that enables data mining and eavesdropping programs.

[24] Hathaway et al.,"The Law of Cyber-Attack."

the United States and Australia have agreed to include cybersecurity cooperation within a defense treaty, declaring that a cyberattack on one country would result in retaliation by both.[25]

Cyberterrorism

As with cyberwarfare, there is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to some activities and damage defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. A notable aspect of this act is its discussion of the "punishment for an offense" entails fines or imprisonment and suggests the offending party is undertaking a criminal act rather than an act of terrorism, which some argue is an act of war if undertaken by a state actor. The CFA is written in such a manner that it could be applied to an individual or groups.

18 U.S.C. 1030(a)(1) finds it illegal for an entity to "knowingly access a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data…with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation." As noted in this section, it appears this statute only pertains to U.S. government networks or networks that may contain restricted data. There is not yet a precedent for an unauthorized computer-supported intrusion rising to the level of being described as a cyberattack.

Some legal analyses define cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[26] The USA PATRIOT Act's definition of "federal crime of terrorism" and reference to the CFA seem to follow this definition. However, these provisions are also criminal statutes and generally refer to individuals or organizations rather than state actors. Naval Post Graduate School defense analyst Dorothy Denning's definition of cyber terrorism focuses on the distinction between destructive and disruptive action.[27] Terrorism generates fear comparable to that of physical attack, and is not just a "costly nuisance."[28] Though a DDoS attack itself does not yield this kind of fear or destruction, the problem is the potential for second or third order effects. For example, if telecommunications and emergency services had been completely dismantled in a time of crisis, the effects of that sort of infrastructure attack could potentially be catastrophic. If an attack on the emergency services system had coincided with a planned real-world, kinetic event, cyber terror or even a Cyber Pearl Harbor event may be an appropriate metaphor. However in this case, the emergency service system itself is most likely not a target, but rather the result of collateral damage to a vulnerable telecommunications network.

[25] See, for example, Lolita Baldor, "Cyber Security Added to US-Australia Treaty," Security on NBCNews.com, 2011, http://www.msnbc.msn.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia-treaty/.

[26] http://www.nato.int/structur/library/bibref/cyberterrorism.pdf.

[27] Dorothy E. Denning. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[28] Serge Krasavin PhD, "What is Cyber-terrorism?," http://www.crime-research.org/library/Cyber-terrorism.htm.

There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying the parameters of what should be construed applicable activities, whether articulating clear redlines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace.

Use of the Military: Offensive Cyberspace Operations

The War Powers Resolution, P.L. 93-148, 87 Stat. 555, sometimes referred to as the War Powers Act, sets the conditions under which the President may exercise his authority as Commander in Chief of U.S. military forces. First, the Resolution stipulates that it be exercised only pursuant to a declaration of war, specific statutory authorization from Congress, or a national emergency created by an attack upon the United States (50 U.S.C. 1541). Second, the Resolution requires the President to consult with Congress before introducing U.S. Armed Forces into hostilities or situations where hostilities are imminent, and to continue such consultations as long as U.S. Armed Forces remain in such situations (50 U.S.C. 1542). Third, it mandates reporting requirements that the President must comply with any time he introduces U.S. Armed Forces into existing or imminent hostilities (50 U.S.C. 1543). Lastly, 50 U.S.C. 1544(b) requires that U.S. forces be withdrawn from hostilities within 60 days of the time a report is submitted or is required to be submitted under 50 U.S.C. 1543(a)(1), unless Congress acts to approve continued military action, or is physically unable to meet as a result of an armed attack upon the United States.

Title 10 of the *United States Code* is the authority under which the military organizes, trains and equips its forces for national defense. Section 954 of the National Defense Authorization Act for Fiscal Year 2012 affirms that "the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution." The House version (H.R. 1540) contained a provision in Section 962 that would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to the Authorization for the Use of Military Force (P.L. 107-40; title 50 United States Code, section 1541 note) outside of the United States or to defend against a cyberattack on an asset of the Department of Defense. Section 941of the House version (H.R. 4310) of the National Defense Authorization Act for Fiscal Year 2013 would have again affirmed the Secretary of Defense's authority to conduct military activities in cyberspace. In particular, it would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on an asset of the DOD. This provision was not in the final version (P.L. 112-239), but a requirement for the Secretary of Defense to provide quarterly briefings to the House and Senate Armed Services Committee on all offensive and significant defensive military operations remained in Section 939.

Another relevant authority through which troops may be dispatched resides in Title 50 of the U.S. Code. Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. 50 U.S.C. 3093 allows the President to authorize the conduct of a covert action if he determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the U.S. national security, which determination shall be set forth in a finding that shall be in writing, "unless immediate action by the United States is required and time does not permit the preparation of a written finding, in

which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made."

50 U.S.C. 413b(e) defines "covert action" as "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." The definition then lists certain exclusions. Traditional military activity, although undefined, is an explicit exception to the covert action definition in 50 U.S.C. 413 as the identity of the sponsor of a traditional military activity may be well known.

According to the Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991, traditional military activities

> include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.

Multiple press sources have reported on a Pentagon plan for "the creation of three types of Cyber Mission Forces under the Cyber Command: 'national mission forces' to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; 'combat mission forces' to help commanders abroad plan and execute attacks or other offensive operations; and 'cyber protection forces' to fortify the Defense Department's networks."[29] These multiservice Cyber Mission Forces numbered under 1,000 in 2013, when DOD announced plans to expand them to roughly 5,000 soldiers and civilians. The target number has since grown to 6,200, with a deadline at the end of FY2016. In early September 2014, a report was provided to Congress from DOD that reportedly stated, "additional capability may be needed for both surge capacity for the [Cyber Mission Forces] and to provide unique and specialized capabilities" for a whole-of-government and nation approach to security in cyberspace.[30]

[29] See http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[30] http://www.defensenews.com/article/20141103/TRAINING/311030018/As-cyber-force-grows-manpower-details-emerge.

Author Contact Information

Catherine A. Theohary
Specialist in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529